Exhibit 68

SW-SEC-SDNY 00006396

Message (Digitally Signed)

From: Quitugua, Eric [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=227693E84BC0400B84364660F692BC85-QUITUGUA, E]
Sent: 10/3/2018 10:17:15 PM
To: Kim, Joe [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=16e76def2a79496eb461e918d4fb3aee-Kim, Joe]; Johnson, Rani [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0ee57945f15e47b3abaa99a59170ad3f-Johnson, Ra]
CC: Brown, Timothy [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a1bcd95116e84d6692dd89f9d55c5b7a-Brown, Timo]
Subject: Security Incident Status Summary
Attachments: smime.p7s

Team,

The following is a list of open security incidents currently in our que and are actively being worked on that you should be aware of.

Business	Title	Summary	Incident Commander	Incident Category	Incident Classification
Cloud	Customer ID mismatch across multiple accounts	Users are reporting seeing errant logs in the Events viewer. This may have resulted from recent code updates	Jason Matthews	Product Security	1-Low
Core	Orion Platform Lacks Proper Access Controls	Improper access controls result in exposure of data	Jeremy Morrill Externally reported by Cisco Systems	Product Security	1-Low
Core	Orion NCM credential exposure	Plaintext credentials for access to configured nodes exposed in HTML source code	David Pluhacek Externally reported by CJD IT Consultancy	Product Security	1-Low
Core	Orion NPM Remote Code Execution	Vulnerability in NPM results in remote code execution	Tim Brown Internally Reported	Product Security	1-Low

We are also currently working through 8 internally reported security incidents that have a classification of 0-Minimal.

You can find additional details of these on Confluence here:
https://cp.solarwinds.com/display/OP/ATTORNEY+WORK+PRODUCT%3A++Incident+Response+Executive+Summaries

solarwinds
Eric Quitugua | Information Security Manager
Office: 512.498.6200